International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
IJISAE
ISSN:2147-6799 www.ijisae.org Original Research Paper

Energy Aware Multi-Modal Homomorphic Security Mechanism for Small Scale Private Cloud Systems

[1]Sindhu V, [2]Rajeswari Mukesh

Submitted: 28/04/2023 **Revised**: 24/06/2023 **Accepted**: 07/07/2023

Abstract: The small scale private cloud systems are widely required for many start-up companies and individual's technology solutions. Comparing to large-scale cloud computing platforms, small scale private networks are expecting limited resources at platform-level, software-level and infrastructure-level. At the same time, people or company requires minimal computation load, energy consumption rate with optimal security features. In this regard, various techniques are developed for supporting small scale systems. Anyhow, the available techniques are not aware of more crucial energy sensitive security procedures. On the scope, the proposed Energy aware Multi-Modal Homomorphic model (EMMH) using light-weight VM assisted encryption techniques. This proposed model assures secure data transmission based on the phases such as data deduplication, Elliptic Curve Cryptography with Digital Signature (ECCDS), Secure Hashing (SHA), random bit inclusions, data extraction and cost validation procedures. The proposed model has been implemented and the results show the proposed model is performing 5% to 12% better than existing techniques.

Index Terms: *Security, Homomorphic encryption, deduplication, Digital Signature, cloud systems and energy cost*

1. Introduction

Cloud computing is virtualized resources can be delivered as a service over the internet. In this environment, users don't need to maintain knowledge or control over the technical infrastructure in the cloud. Instead of having highest resources (software, infrastructure and platform), lowest cost can be spent for buying high performance computers, drives and platforms with maximum availability modes. In that case, user can buy required storage, processors, software and other services at a very optimal cost through cloud computing environment. Particularly, this kind of provisions are more affordable for improving small scale private cloud networks and big company.

It can also provide millions of servers, high speed computing environment, refrigeration, and maintenance technicians in cloud computing, you can get the fastest service possible. Large companies are managing huge data centers to provide cloud computing services. The current technological developments are made in hardware and software. Different types of cloud networks present such as public domain, private domain and hybrid domain (platform, software and infrastructure).

These types of services are adapted in recent technologies that rely on the web to satisfy computational needs. Cloud computing services are provided through online mode and common business application that can be accessed based on demands. Public cloud describes cloud computing with resources and costs are shared on fine grained utility computing, where web application or web services are delivered over the internet from a third party providers. Services are provided dynamically on a self-service basis. Private deployment model is deployed for as the internal cloud computing services for the companies behind the corporate related firewall. Organization can control the data is being held and can build the organization infrastructures. A hybrid cloud environment involves multiple internal and external service providers typically for most enterprises.

Among these cloud deployment models, private cloud services are given for hardware and software as per the requirements of a user. Any type of organization can use private cloud services with single affinity data stored in the cloud. Similarly, the organization can find hardware services with physical systems and virtual systems on which the cloud is developed. Private cloud environment can also be used with multiple applications or single cloud based application. For example, websites, back end services, virtual infrastructures, machine learning applications, and various databases.

In this case, small scale private cloud services are more expected nowadays within a lower-end organizations and startups. The small scale private cloud models are deployed such as shared private cloud model, dedicated private cloud model and dynamic private cloud model.

The shared cloud services with variable demand based solutions are used for small scale business units that are based on service offerings, account management and data centers. It expects an internal profit to take over infrastructures, services and platforms made available for user's demands. In the same manner, dedicated private cloud

[1]*Research Scholar, Bharathiyar university, Coimbatore, India*
sindhuvcsmop@gmail.com
[2]*SRM Institute of Science and Technology, Ramapuram, Chennai, India*
mukeshrajeswari@gmail.com

depends on standardized services and assets that can be deployed for valid users at a lower cost model. At the end, dynamic private cloud services migrate through various policies to the complete cloud service requirements. Different types of advantages are expected in small scale private cloud such as high speed, data privacy, customizable and reliability.

Under this cloud environment, security and data management are significant tasks to assure user data protection. Cyber security and information security are emerging as major needs for large companies to improve security features in the data centers. In private cloud, security concerns are more since customer data need to be followed under standardized rules. In this regard, user expects customized and reliable security support from cloud service providers.

Cloud is a shared internet environment among various types of users with required features. The security is a major need to protect user data that can be attained via stream chiper (bit-wise encryption) or block chiper (data block encryption) techniques. In block cipher technique, user data is formed as a block size of 64 bits or 128 bits with required key bits. This can be implemented in symmetric mode or asymmetric mode. Mostly, the current day schemes are using Data Encryption Standard (DES) or Advanced Encryption Standard (AES) under block chiper mode. In stream cipher techniques, chain of bits is operated for encryption. Anyhow, more complexity is required for recent protection mechanisms. In this manner Homomorphic encryption (HE) is invented to encrypt the data and post processing of encrypted data in its form.

HE is a type of encryption that allows computation of encryption data in its actual format. In short, HE assures the operations on encrypted data and decrypting the result is equivalent to performing the same kind of operations without any further encryption. HE is not only to protect data owners yet has data privacy concerns around the data for customers with valuable intellectual properties. Homomorphic encrypted data can be assumed that owner does not see the user's private data and therefore cannot be compromised. In this case, interconnection between data and model owners is not required to perform the calculation.

HE can be used for small scale private cloud systems and it can establish a high level of data security without breaking computation process or application services. The organizations can ensure data privacy while deriving security principles for sensitive data. Applications of HE include cloud workload security, aggregation analytics, privacy-preserving encryption, authentic encryption, secure information supply chain integration, and secure automation.

Joshi B et al. [1] proposes homomorphic encryption-based security and privacy preserving techniques. The work is about third party's hosting the cloud data in cloud network and the issues in security metrics, privacy and safety measures. On the base, this work is identifying and comparing different types of homomorphic encryption schemes to save the data among third parties. Munjal K et al. [2] proposes healthcare industry related homomorphic encryption and systematic based homomorphic encryptions. In this regard, cloud not only secures the data yet helps to store employees' data, patient data in places like industrial, hospital, medical through this research.

Joseph M et al. [3] proposes data security with hybrid optimization and HE encryption. This concept is proposed to data security in cloud computing. This method proposes against the cloud data theft by third parties and secures the data via HE functions. Hidayat et al. [4] proposes data transformation techniques and encrypts the data during transmission in cloud networks. This concept is used with AES algorithm to encrypt the data transmission in the cloud network. As cloud is vast service area where the cloud data are hosted among third parties, it is very important to determine safety issues and potential problems, on secure data transfer policies.

As many existing techniques are using HE and other encryption techniques, the data security problem can be solved in various manner. However, the effective analysis of energy wastages and computation load among cloud processing points are not conducted properly by any available techniques. This is considered as major research problem and the proposed EMMH model is motivated and contributing the following solutions against various cloud security issues and data security issues.

- Removal of duplicated data (deduplication) and malicious data from HE
- Data on transit and Data storage security principles
- Authentic and Energy-Aware HE model
- EMMH-IDS framework for effective cloud data validations
- Secure data decryption model

This article is organized as literature analysis in section 2. Section 3 provides the EMMH proposed model and technical procedures. Section 4 shows the cloud testbed descriptions and implementation details. Section 5 provides concluded information and future work.

2. Literature Review

The related techniques used for understanding the security models of cloud model are given below. Liu J et al. [5] proposed multiple keywords rank search encryption and wild keyword data sharing in cloud computing. This method proposed for effective searching on encrypt data's. The most crucial concept of the work about multi-keyword ranking searchable encryption to search and ranking on the sever side. This method sometimes may not be able to access some keywords. So this work says using Multi-Keyword Ranked Searchable Encryption multi keywords (MRSW) method. This method is advanced technology so easy to access keywords with searching data yet it was not energy efficient.

Aljawarneh et al. [6] proposed a conceptual safe and secure framework for (CC) cloud computing problems. Then practitioner's perspectives to address client concerns. Data safety in cloud computing also shown to raise awareness of measures to ensure software security of cloud computing. Finally, they are using conceptual safety and security method help to potential development of cloud software security architecture to address numerous issues in cloud safe and security at different architectural levels.

Choudhary S et al. [7] proposed access control method on searching cloud data randomly. Through this, this model controls unauthorized user access on information in cloud computing platforms. Budhwani T et al. [8] proposed secure data searching in cloud models. In this work, users' data are store in cloud and provided for authorized people only. Cloud safety and security risks, users access controls, then network security are the searching methodologies used for securing cloud data.

Kara M et al. [9] proposed a totally homomorphic encryption related on numerical fragmentation and ElGamal encryption. This concept is used to perform smart city development, city side every day activities, expanding object oriented communities' data's collect and share sensitive data's in cloud computing.

Kiesel et al. [10] proposed various use cases for implementing potential-level homomorphic encryption techniques for securing the cloud systems. According to these use cases, this model gave the possibilities of various potential issues and appropriate solutions using homomorphic encryption techniques. In addition, the possible and valid use cases can be acquired under cloud security constraints. In the same manner, Li et al. [11] proposed multi-key generation policies and digital checksum computations under homomorphic models for securing cloud data. Particularly, these works were targeting data confidentiality issues and data integrity issues in cloud computing platforms.

In Kara et al. [12] one-digit checksum generation and cloud-based homomorphic encryption algorithm (E: A). In this approach, each data block was secured using single bit checksum validation at the destination point. In addition, the homomorphic encryption and one bit validations are operated in cloud systems. The novel approach provided useful security solutions for runtime data transmission as it was one-bit checksum. Anyhow, this is not complex for effective attackers.

Jung et al. [13] developed the acceleration process of homomorphic encryption technique by analyzing the cloud architectures and infrastructures. In this mechanism, the novel idea was created to map the security procedures of homomorphic encryption and internal cloud components with their architecture patterns (E: B). This work stated the importance of architecture analysis and improvement of encryption cycles in cloud. However, this model was not any specific security issues.

Bhowmik et al. [14] proposed isomorphic encryption functions with trained artificial neural networks and mealy state machines. The combination of isomorphic functions and artificial neural network worked well to learn the system behavior and initiate encryption procedures on respective data (E: C). At the same time, this mechanism initiates state flow observation and state machine transitions through mealy model. This idea worked in optimal manner yet the complexity was expected to be limited.

Based on real-time security issues, multiple homomorphic solutions are providing by existing techniques [15][16]. At the same time, the identification of proper and distributed homomorphic security system for small scale private cloud systems does not exist around the existing models. This is considered as major problem since the need for more optimal security is essential for supporting start-ups and individual's platform. In this regard, the proposed EMMH model has been created and implemented. The technical details and the results are illustrated in section 3 and 4 respectively.

3. Proposed Model

Small scale private cloud networks can be implemented to manage low-level field information such as sensor data and other observations. The data can be collected by small scale private cloud networks are assumed to be sensor data, real-time market data, medical data or any customer data. As small scale companies are limited to cost and computing capabilities, the need for more resilient and optimal set of data encryption principles is mandatory. Based on the EMMH model, equations (1)→(3) show the data collection principle [17][18].

Data collection and energy monitoring model,

$$cm = \begin{cases} p(si,ti) \ , ch(d) \geq 1 \\ f(si,ai) \ , sd(d) \geq 1 \\ 0 \ , Null \end{cases} \tag{1}$$

$ch(d)$: $Channel\ Data$

$sd(d)$: $Data\ on\ storage$

Data Packet on Channel,

$$p(si,ti) = \sum_{i=1}^{l} Data\ (\mathrm{Pr}(i)\ , Packet(i), f, ti) \tag{2}$$

si, ti: $Segment\ identifier\ and\ timestamp$

$Pr(i)$: $Protocol\ Attributes$

$Packet(i): Data\ as\ Packet$

$f: flow\ type\ (unidirectional/bidirectional)$

$ti: Timestamp$

$$f(si, ai) = \sum_{i=1}^{l} D\_Block\ (\text{f\_a}(i), s\_a(i), dti) \qquad (3)$$

$f\_a(i): file\ attributes$

$s\_a(i): Data\ block\ attributes$

$dti: time\ of\ data\ deployment\ in\ a\ cloud\ storage$

Based on the data collection models, the data on cloud can be considered as either "data on transit" or "data on storage". Unlike other existing models, this proposed EMMH gets both type of data into security perimeter. Similarly, energy model is created under proposed EMMH principle as given in equation (4) [19][20].

$$em = \begin{cases} ch(d)\ , eS(d) \le eTS(d) \\ sd(d)\ , eA(d) \le eTA(d) \\ -1\ \ , Energy\ Error \end{cases} \qquad (4)$$

$eS(d): energy\ served\ at\ communication\ nodes\ for\ packet\ management$

$eTS(d): Threshold\ energy\ on\ packet\ management$

$eA(d): energy\ served\ for\ data\ block\ access\ at\ cloud\ storage\ points$

$eTA(d): Threshold\ energy\ on\ cloud\ data\ access\ tasks$

The overall system design of EMMH model has been illustrated in figure 1. As given in figure 1, the proposed model has been developed from the phase of data collection and data modelling procedures. The proposed model assumes that the data are collected from various edge (end) devices such as sensors, mobile devices, computers, or any other gadgets. In the next level, this model considers the procedures of data extraction (packets and files in storage) and analysis. Under this phase, packets are extracted using packet filtering tool and stored data are analyzed using file property extractor tools [21][22].

In this model, the second step is more important to get the data ready to observe the duplicate or compromised data (packet). Generally, packets are extracted based on their layer-wise attributes and priorities.

In addition, files stored in cloud storages are identified as a collection of attributes and permissions. Based on these procedures, the following properties are achieved in proposed EMMH model. [23][24]

- Data deduplication [Packets and File Data]
- Malicious events [Packets and File insertions]

According to the descriptions, procedures (1)→(4) are illustrated as given below.

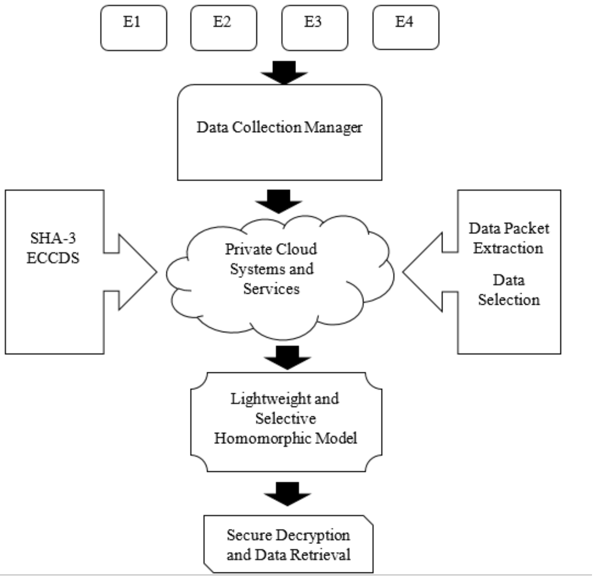

Fig. 1. Proposed EMMH Model

- P1: Multi-Channel Data Collection and Energy Based Distribution
- P2: VM Modelling and Attribute Extraction
- P3: VM Based IDS Engine
- P4: Authenticated and Multi-modal Homomorphic Model

In this manner, multi-channel data collection and energy based data distribution are activated based on the data collected from edge devices [25][26][27].

P1: Multi-Channel Data Collection and Energy Based Distribution

```
Input: $Data\ from\ Edge\ points, E1 \dots En$
Output: $d(cm, em) \rightarrow Di: VMi$
Begin
1: Get all $p(si, ti): f(si, ti) \rightarrow Di\ at\ VMs$
2: Call data model function at $VM^{i}$ :
        2.1: For all, $p(si, ti): VM^{i}$, call packet extraction function
            $ep(si, ti) = Data\ (\Pr(i)\ , Packet(i), f, ti)$
        2.2: For all, $f(si, ti): VM^{i}$, call data access principle function
            $ep(si, ti) = D\_Block\ (f\_a(i), s\_a(i), ti)$
3: Call energy model function and computation load evaluation function
        3.1: For all, $p(si, ti): f(si, ti): VM^{i}$, call energy evaluation function
            $Lc(si, ti) = Ec + P(Nc, dt) for\ all\ i : Ec: Energy\ cost$
                                        $Nc: Node\ Cost$
        3.2: Set $Lc(si, ti): Di$ classes and redistribute the load optimally
4: Check all data on VMs and cloud communication points
5: Find Data errors and energy violations
6.Redo for all data on cloud systems
End
```

P2: VM Modelling and Attribute Extraction

```
Input: $Di: VM \rightarrow Network$
Output: $A(p(si, ti): f(si, ti))$
Begin
1: Set physical machines with $k$ number of VMs
2: Set $Network \rightarrow VM(m, p, i)$: m-memory ;p-processor; i-VM identifier
3:  Get $p(si, ti): f(si, ti)$ at each VM
    3.1: Extract $p(si, ti): f(si, ti)$ features
    3.2: If data→ $p(si, ti)$:
                    Number of data segments & identifiers
                    protocol type: source and destination address
                    Security certificates and data types
                    Timestamp and compromised status
    3.3: If data→ $f(si, ti)$:
                    Number of file segments & logical blocks
                    file type: permissions: security features
                    Security certificates and file types
```

```
                                   Timestamp and ownership
                                   File modification status and access controls
                                   Access log
4: Call 3.2 or 3.3 based on data modes
5: Call attribute analyser as packet capturing function or file attribute analyser
6: Redo for all data
End
```

Each edge device has its data patters and energy expectation levels. Similarly, the cloud environment has its own set of Virtual Machines (VMs) to form a collective cloud resource [28][29]. Based on these VM assisted private cloud environment, each VM has its significant data as either packet or its own files. According to the model, the VMs are consuming varying order of energy costs and node costs. The details are illustrated in procedure 1. In addition, procedure 2 illustrates the steps of attributes extraction details for both transmitted data and stored data. As per the needs, the procedure 2 extracts the packet details with notable feature as given below [30].

- Number of data segments & identifiers
- protocol type: source and destination address
- Security certificates and data types
- Timestamp and compromised status

Similarly, the stored data or files are extracted for understanding the given details.

- Number of file segments & logical blocks
- file type: permissions: security features
- Security certificates and file types
- Timestamp and ownership
- File modification status, access log and access controls [31]

```
P3: VM Based IDS Engine
Input: $A(p(si,ti):f(si,ti))$
Output: Alert on $A(p(si,ti):f(si,ti))$
Begin
1: Get all $A(p(si,ti):f(si,ti)) -\rightarrow VM^{i}$
2: Classify $A(p(si,ti))$ $and$ $A(f(si,ti)) -\rightarrow VM^{i}$
          2.1: For all, $A(p(si,ti))$  [Wireshark tool]
                 $IDS\_R = f(R, p(si,ti), t))$
                 Generate IDS_R Report at VM buffer, P[k]
                  Raise alert for malicious events
          2.2: For all, $A(f(si,ti))$
                 $IDS\_R = f(R, f(si,ti), t))$
                 Generate IDS_R Report at VM buffer, f[k]
                 Raise alert for malicious blocks
3: Get legitimate data from P[k] and f[k].
4: Assign all $A(data,i)$ in to secure buffer, $S(data,h)$for encryption
5: Initiate periodic refreshment on buffer
End
```

The given details are significant to observe the duplicate data or malicious data in cloud.

```
P4: Authenticated and  Multi-modal Homomorphic Model
Input: $S(data, h)$
Output: $E\_H(S(data, h))$
Begin
1: Get all $S(data, h)$; $data$: $Intrusion\ controlled\ data$; $h$: $buffer\ hash\ values$
2: Call ECCDS (256 bits) in all $VM^i$
        2.1: For all, $S(data, h)$ [Phase 1]
            $e(S(data, h), i) = ECCDS[D] + Nonce + Timestamp$
        2.2: For all $e(S(data, h), i)$ [Phase 2]
            $Sha_{3\{e(S(data,h),i)\}} = H\big(e(S(data, h), i)\big) + Rb$
            Rb: Random Binary bits [homomorphic]
3: Set VM local memory and maintain → $Sha_{3\{e(S(data,h),i)\}}$
4: Process or transmit the data in the cloud
5: Decrypt the data based on valid user demands
6: Redo for all VMs
End
```

The execution of procedure 1 and 2 shows the observation of cloud data collection and attribute extraction respectively. In the same manner, procedure 3 shows the VM based Intrusion Detection System (IDS) engine to identify the cloud data irregularities created by any internal or external malicious nodes. Due the novel steps of this procedure 3, each VM has the ability to classify the needful data in to encryption phase no other malicious events. This save time, computation load and energy spent in each VM [32][33].

According to the observations of procedure 3, procedure 4 initiates optimal and energy controlled HE with authentication procedures. In this method, each packet or data has been authenticated using Secure Hashing (SHA) and encrypted using ECCDS functions. Based on this procedure, each data has been encrypted and authenticated twice to increase the information security. In this case, HE principles are executed by concatenating random number (bits) and data nonce in encrypted data (cipher text) [34][35].

Proposed HE has been implemented in EMMH models through novel approaches unlike other conventional and existing functions. This proposed method has achieved significant level of security around distributed small scale cloud VMs. In extend, this EMMH has provided more convenient and de-duplicated HE solutions. The technical features are implemented and results are observed as given in section 4.

4. Results and Performance Comparison

The proposed model has been configured and implanted in cloud simulation tool. The cloud simulation tool is used to deploy cloud environment and VMs with its respective characteristics. This work creates 5 VMs in each physical machine of cloud environment. In addition, this cloud model has totally 15 physical machines in the field. In the same manner, each VM has the feature of data gatherings, intrusion rule engine and homomorphic functional units [36][37]. The proposed functions and homomorphic functions are implemented using python 3.0 with its security packages. The proposed model and the existing models [E: A, E: B and E: C] are compared in this deployed testbed environment using the following performance metrics.

- Encryption Time (milliseconds, msec)
- Computation overhead
- Energy spent on data types
- Secure data rate
- Memory complexity in VM
- Data extraction rate and Optimal security cost

As discussed, E: A is a security technique used for enabling cloud based homomorphic encryption and one-bit checksum computation procedures.

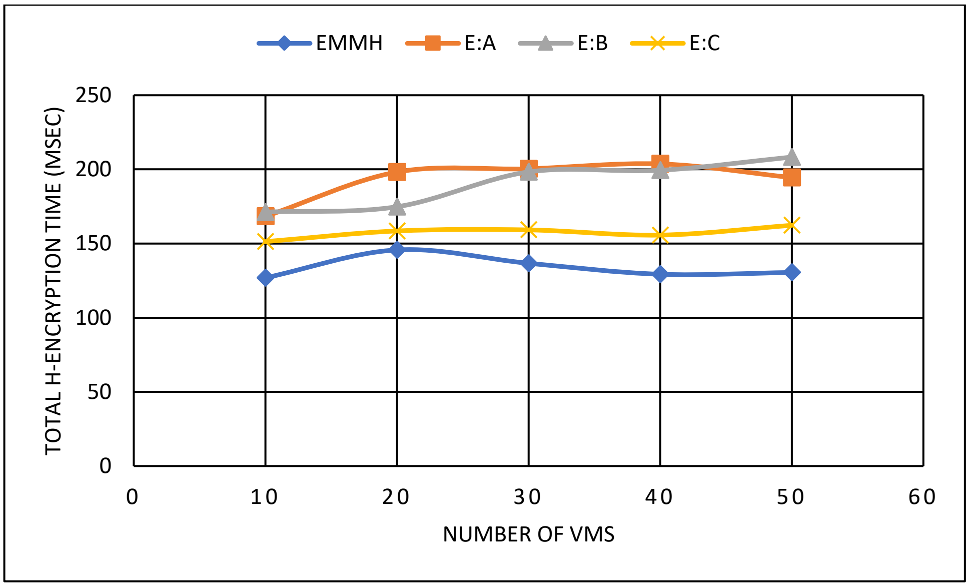

Fig. 2. Time Complexity

In the same way, E: B is an existing technique used to implement acceleration procedures of homomorphic encryption based on cloud architectures. The third existing technique used for performance comparison is E: C, used to implement Artificial Neural Network (ANN) based isomorphic encryption.

As given in figure 2, time complexity is measured against the number of VMs in cloud. In this comparison, the proposed model has been compared with existing techniques as mentioned. This comparison reveals that the proposed EMMH model is getting optimal time complexity (between 120 milliseconds (msec) and 149 msec) against changing number of VMs from 10 to 50. The reason behind this performance is the EMMH uses enhanced attribute extraction on both online and offline data.

In this regard, the EMMH reduces the malicious events in to encryption procedures for reducing the time. At the same time, the exiting techniques are generally handling the data in to encryption techniques. Anyhow, E: C uses ANN for encryption tuning functions and produces little time complexity compared to E.B and E: A.

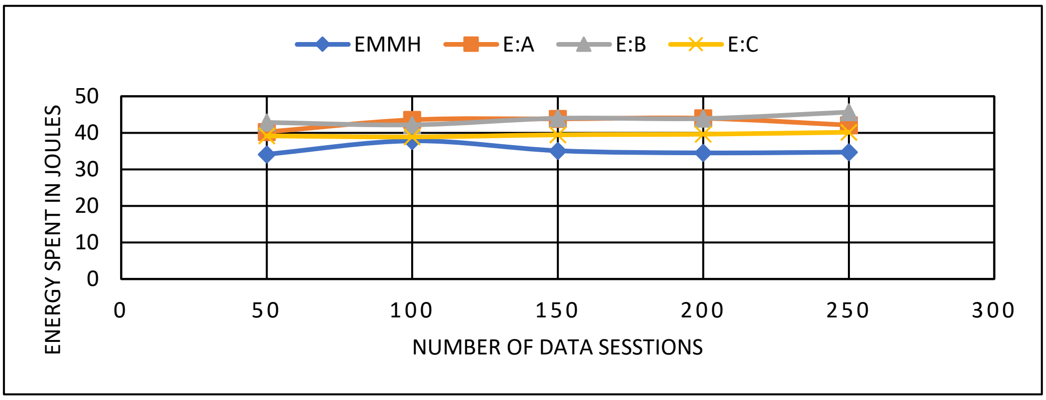

Fig. 3. Energy Complexity

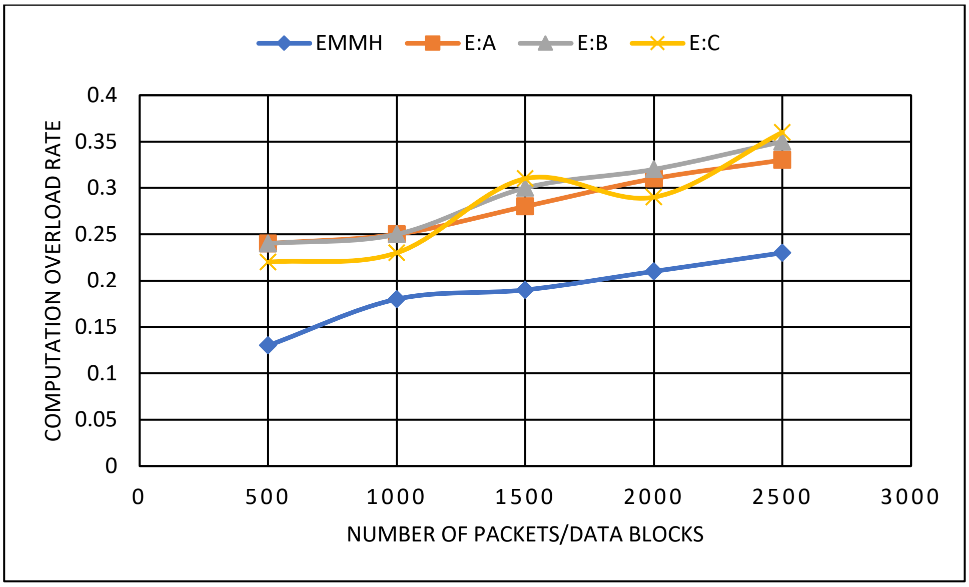

Fig. 4. Computation Overhead

Figures 3 and 4 are relative performance observations in terms of computation load and energy spent during the procedure executions. These two parameters are directly proportional to each other's, since the excess computation load increases energy spent at each node directly. In this comparison, the proposed model consumes less energy and computation load (35 Jules and 0.22) since it is using homomorphic encryption functions on de-duplicated (reduced data) data by removing malicious events. At the same time, others are performing at moderate range only.

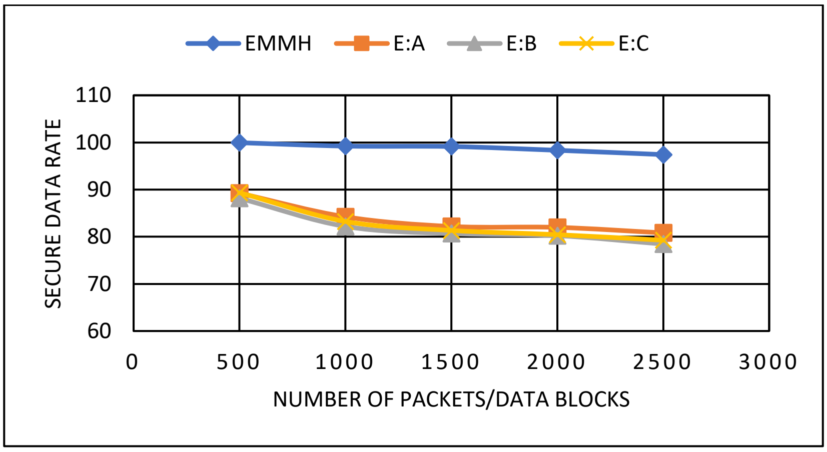

Fig. 5. Secure Data Transmission

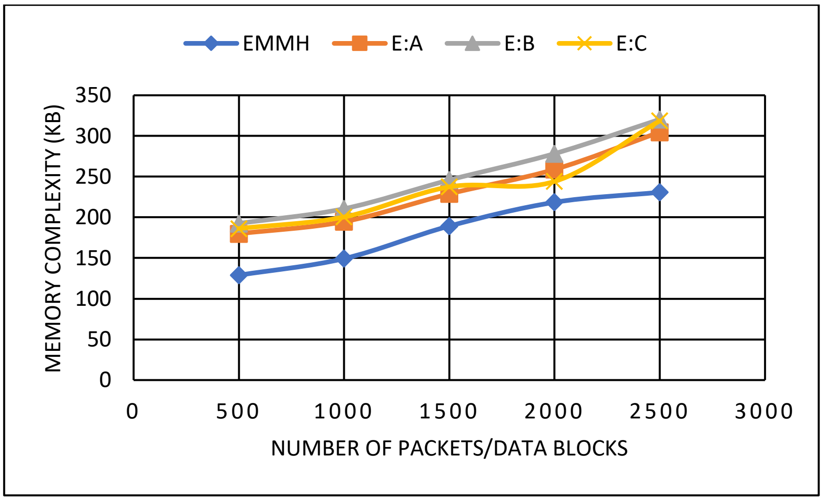

Fig. 6. Memory Complexity

Figure 5 shows the performance of systems' security level in terms of secure data rate against number of packets or data blocks. Secure data rate shall be calculated from the ratio between the total packets (data) and the packets (data) successfully transferred among malicious presents. As the number of data or packet increases, the secure data rate gradually decreases against the attacker events.

As given in figure 5, EMMH varies from 99.8% to 97.6% of secure data rate. In this comparison, other existing techniques are not effective against threats. Since the proposed model uses R-AES and R-MAC for enabling authenticated encryption functions with homomorphic encryption functions, the security level is increased against malicious events.

Figure 6 illustrates the memory required at each node for security procedures of EMMH, E: A, E: B and E: C. The memory required to store the procedures and the cipher text are illustrated in Kilo Bytes (KB). In this comparison, the proposed model and existing techniques are closely competing each other. Anyhow, EMMH requires 150 KB to 220 KB of memory space to hold the function codes. On the other side, the existing techniques as consuming more memory space since they don't have any data reduction policies and de-duplication procedures.

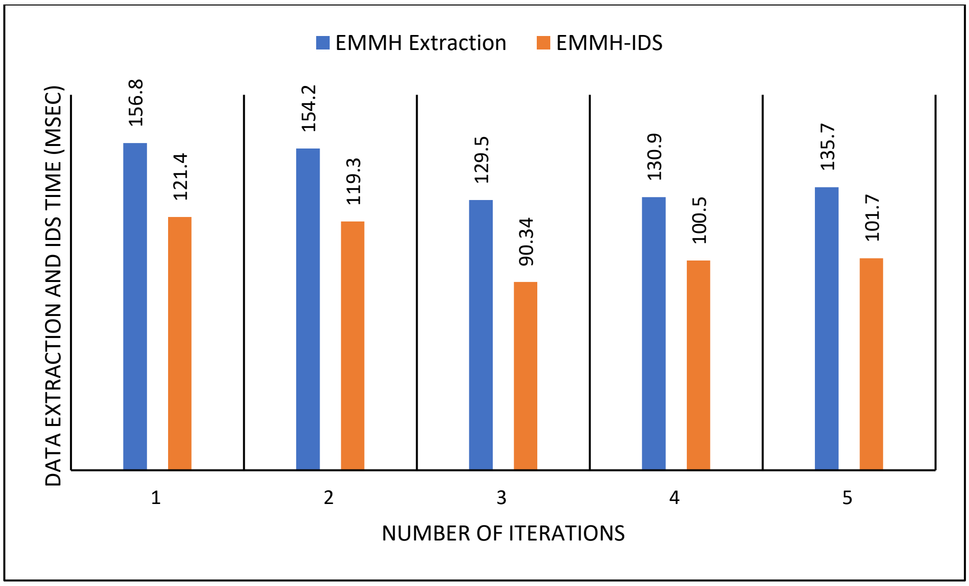

Fig. 7. Data Extraction Time of EMMH

Figure 7 gives the time taken to extract the data from packets or files by proposed EMMH model for multiple iterations. According to this observation, there are two main operations required that are available in existing techniques. They are EMMH packet or data attributes extraction and EMMH Intrusion Detection System (IDS) procedures. These procedures are more significant to build de-duplicated and pre-processed data streams in to EMMH model and homomorphic encryption solutions. In this experiment, data extraction phase needs time between 130.9 msec and 156.8 msec. On contrast, time taken to complete the IDS procedures falls between 90.34 msec and 121.4 msec. Anyhow, these time factors are not crucial to provide restricted homomorphic encryption solutions at optimal energy costs and time costs.

5. Conclusion and Future Work

The effective application of homomorphic encryption technique at optimal energy cost was the main motive of this proposed EMMH model. In this work, the proposed EMMH model has been created with appropriate data model, private cloud network model, distributed VM configuration model, R-AES, R-MAC, homomorphic functions and novel attributed analysis (packets and file data). Through these novel procedures, the proposed technique achieved better energy consumption rate, time optimization, memory utilization cost and optimal secure data rate against the existing techniques such as E: A, E: B and E: C. However, the proposed EMMH model was not optimized for handling different types of attacks under this scenario. It was only considered for handling rule based and content based malicious events in this experiment. This can be solved in future.

References

[1] B. Joshi, B. Joshi, A. Mishra, V. Arya, A. K. Gupta, et al., "A comparative study of privacy-preserving homomorphic encryption techniques in cloud computing," *International Journal of Cloud Applications and Computing (IJCAC)*, vol. 12(1), pp. 1–11, 2022.

[2] K. Munjal and R. Bhatia, "A systematic review of homomorphic encryption and its contributions in healthcare industry," *Complex & Intelligent Systems*, vol. 3, pp. 1–28, May 2022.

[3] M. Joseph and G. Mohan, "Design a hybrid optimization and homomorphic encryption for

securing data in a cloud environment," *International Journal of Computer Networks and Applications (IJCNA)*, vol. 9(4), pp. 387–95, July 2022.

[4] T. Hidayat, D. S. Franky and R. Mahardiko, "Forecast analysis of research chance on AES algorithm to encrypt during data transmission on cloud computing," In 2020 2nd International Conference on Broadband Communications, Wireless Sensors and Powering (BCWSP), IEEE, pp. 163-166, September 2020.

[5] J. Liu, B. Zhao, J. Qin, X. Zhang and J. Ma, "Multi-keyword ranked searchable encryption with the wildcard keyword for data sharing in cloud computing," *The Computer Journal*. vol. 66(1), pp. 184–96, January 2023.

[6] S. A. Aljawarneh and M. O. Yassein, "A conceptual security framework for cloud computing issues," *International Journal of Intelligent Information Technologies (IJIIT)*, vol. 12(2), pp. 12–24, April 2016.

[7] S. Choudhary and N. Singh, "Analysis of security-based access control models for cloud computing," *International Journal of Cloud Applications and Computing (IJCAC)*, vol. 12(1), pp. 1–9, January 2022.

[8] T. Budhwani, P. Tejaswini, A. Chowdhury, D. B. Bolli, F. Uddin et al., "An analysis of cloud security," *Int. Res. J. Eng. Technol*., 9(2), 2022.

[9] M. Kara, A. Laouid, M. A. Yagoub, R. Euler, S. Medileh et al., "A fully homomorphic encryption based on magic number fragmentation and El-Gamal encryption: Smart healthcare use case," *Expert Systems*, vol. 39(5), pp. e12767, June 2022.

[10] R. Kiesel, M. Lakatsch, A. Mann, K. Lossie, F. Sohnius et al., "Potential of homomorphic encryption for cloud computing use cases in manufacturing," *Journal of Cybersecurity and Privacy*, vol. 3(1), pp. 44–60, February 2023.

[11] X. Li, H. Li, J. Gao and R. Wang, "Privacy preserving via multi-key homomorphic encryption in cloud computing," *Journal of Information Security and Applications*, vol. 74, pp. 103463, May 2023.

[12] M. Kara, A. Laouid, M. Hammoudeh and A. Bounceur, "One digit checksum for data integrity verification of cloud-executed homomorphic encryption operations," *Cryptology ePrint Archive*, 2023.

[13] W. Jung, E. Lee, S. Kim, J. Kim, N. Kim, et al., "Accelerating fully homomorphic encryption through architecture-centric analysis and optimization," *IEEE Access*, vol. 9, pp. 98772-89, July 2021.

[14] A. Bhowmik and S. Karforma, "Isomorphic encryption and coupled ANN with Mealy machine: a cutting edge data security model for cloud computing environment," *Knowledge and Information Systems*, vol. 65(1), pp. 133–62, January 2023.

[15] C. Rupa and M. A. Shah, "Novel secure data protection scheme using Martino homomorphic encryption," *Journal of Cloud Computing*, vol. 12(1), pp.1–2, December 2023.

[16] C. Rout, S. Sethi, R. K. Sahoo and J. Chandrakanta Badajena, "Empirical analysis of the impact of homomorphic encryption on cloud computing," *Intelligent Systems and Applications: Select Proceedings of ICISA* **2022**, vol. 1, pp. 107–20, January 2023.

[17] N. Vijayaraj and S. Arunagiri, "Demultiplexer design using photonic crystal ring resonator with high quality factor and less footprint for DWDM application," *Opt Quant Electron*, vol. 54, pp. 465, 2022. https://doi.org/10.1007/s11082-022-03817-2

[18] Nivethitha, et.al., "Conceptual approach on smart car parking system for industry 4.0 internet of things assisted networks", in *Measurement: Sensors*, Vol. 24, December 2022, https://doi.org/10.1016/j.measen.2022.100474

[19] P. Elumalaivasan et. al., "CBIR- Retreival of Images using Median Vector Algorithm", *International Conference on Green Computing, Communication and Conservation of Energy, ICGCE 2013*, pp. 1–5, 2013,

https://doi.org/10.1109/ICGCE.2013.6823389

[20] S. Suthir and S. Janakiraman, "SNT Algorithm and DCS Protocols coalesced a Contemporary Hasty File Sharing with Network Coding Influence", *Journal of Engineering Research*, vol. 6, issue 3, pp. 54–69, 2018.

[21] E. N. Oh, M. R. Baharon, S. M. Yassin, A. Idris and A. MacDermott, "Preserving data privacy in mobile cloud computing using enhanced homomorphic encryption scheme," *Journal of Physics: Conference Series*, vol. 2319, no. 1, pp. 012024, August 2022. IOP Publishing.

[22] M. M. Salim, I. Kim, U. Doniyor, C. Lee and J. H. Park, "Homomorphic encryption based privacy-preservation for iomt," *Applied Sciences*, vol. 11(18), pp. 8757, September 2021.

[23] C. Jayashri, et. al., "Big data transfers through dynamic and load balanced flow on cloud networks", *3rd IEEE International Conference on Advances in Electrical and Electronics, Information, Communication and Bio-Informatics*, pp. 342–346, 2017. https://doi.org/10.1109/AEEICB.2016.7538376.

[24] W. Ren, X. Tong, J. Du, N. Wang, S. C. Li, et al., "Privacy-preserving using homomorphic encryption in mobile IoT systems," *Computer Communications*, vol.

165, pp. 105-11, January 2021.

[25] S. Suthir, et. al., “A contemporary network security technique using smokescreen SSL in huddle network server,” *2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)*, pp. 673–676, 2016. https://doi.org/10.1109/AEEICB.2016.7538376

[26] S. J. Mohammed and D. B. Taha, “Performance evaluation of RSA, ElGamal, and Paillier partial homomorphic encryption algorithms,” *In 2022 International Conference on Computer Science and Software Engineering (CSASE)*, IEEE, pp. 89–94, March 2022.

[27] H. Fang and Q. Qian, “Privacy preserving machine learning with homomorphic encryption and federated learning,” *Future Internet*. vol. 13(4), pp. 94, April 2021.

[28] Vijayaraj Nivethitha and A. Sivasubramanian, “Intensification and interpretation of performance in 5G adopting millimeter wave: a survey & future research direction,” *International Arab Journal of Information Technology*, vol. 20, No. 4, July 2023.

[29] Taha Junaid, et.al., “A comparative analysis of transformer based models for figurative language classification,” *Computers and Electrical Engineering*, vol. 101, July 2022, https://doi.org/10.1016/j.compeleceng.2022.108051

[30] S. A. Sheik and A. P. Muniyandi, “Secure authentication schemes in cloud computing with glimpse of artificial neural networks: A review,” *Cyber Security and Applications*, vol. 1, pp. 100002, December 2023.

[31] C. L. Stergiou, E. Bompoli and K. E. Psannis, “Security and privacy issues in iot-based big data cloud systems in a digital twin scenario”, *Applied Sciences*, vol. 13(2), pp. 758, January 2023.

[32] H. Yin, W. Zhang, H. Deng, Z. Qin and K. Li. “An attribute-based searchable encryption scheme for cloud-assisted IIoT” IEEE Internet of Things Journal, February 2023.

[33] M. Kara, A. Laouid, A. Bounceur, M. Hammoudeh, M. Alshaikh, “Perfect Confidentiality through Unconditionally Secure Homomorphic Encryption Using OTP With a Single Pre-Shared Key,” *Journal of Information Science & Engineering*, vol. 39(1) January 2023.

[34] H. Kang and J. Deng, “A cross encryption scheme for data security storage in cloud computing environment,” *Int. J. Internet Protocol Technology*, 16(1) pp. 1, 2023.

[35] D. Prabhu and Vijay Bhanu, “Privacy preserving steganography based biometric authentication system for cloud computing environment”, *Measurement: Sensors Journal*, vol 24, December 2022. https://doi.org/10.1016/j.measen.2022.100511

[36] D. Prabhu and Vijay Bhanu, “Design of multiple share creation with optimal signcryption based secure biometric authentication system for cloud environment”, *International Journal of Computers and Applns.*, 44(11), pp. 1047–1055, 2022. https://doi.org/10.1080/1206212X.2022.2103890

[37] C. Vijayalakshmi, et. al., “A survey on solving dilemmas of adapting blockchain in different applications”, 1st International Conference on Recent Advances in Manufacturing Engineering Research, ICRAMER 2021, AIP Conference Proceedings, vol. 2460, pp. 070011, 2022. https://doi.org/10.1063/5.0095701

[38] Archana, M., Kavitha, S., & Vathsala, A. . (2023). Auto Deep Learning-based Automated Surveillance Technique to Recognize the Activities in the Cyber-Physical System. International Journal on Recent and Innovation Trends in Computing and Communication, 11(2), 35–42. https://doi.org/10.17762/ijritcc.v11i2.6111

[39] Anna, G., Hernandez, M., García, M., Fernández, M., & González, M. Optimizing Course Recommendations for Engineering Students Using Machine Learning. Kuwait Journal of Machine Learning, 1(1). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/104

[40] Dhabliya, D. (2021). Delay-tolerant sensor network (DTN) implementation in cloud computing. Paper presented at the Journal of Physics: Conference Series, , 1979(1) doi:10.1088/1742-6596/1979/1/012031 Retrieved from www.scopus.com